CLAIMS

1. A method for managing secure communication remotely between a device coupled to a gateway and a server, the method comprising:

generating, by the server, a unique identifier based on encrypted data received from the gateway;

authorizing, by the server, the gateway for communicating with the server based on the unique identifier;

providing, by the server, a credential token associated with the gateway for use in communications between the gateway and the server;

generating, by the server, a key associated with the device for communicating between the device and the server;

authorizing, by the gateway, the device for communicating with the server based on the generated key associated with the device;

accessing, by the server, data from the device based on the generated key; and

managing, by the server, the communication between the device and the server remotely.

2. The method according to claim 1, wherein generating the unique identifier based on encrypted data received from the gateway comprises:

receiving an encrypted data from the gateway;

decrypting the encrypted data;

validating and storing decrypted data; and

generating the unique identifier based on the validated data.

3. The method according to any of the preceding claims , wherein a plurality of devices couple to the gateway.

4. The method according to any of the preceding claims , wherein the server is in communication with a plurality of gateways.

5. The method according to any of the preceding claims , wherein the server comprises a pool of the unique identifiers.

6. The method according to any of the preceding claims, wherein the coupling of the device and the gateway is provided by physical ports or wireless communication.

7. The method according to any of the preceding claims , wherein the gateway is encrypted.

8. The method according to claim 7, further comprising creating and storing a decryption key associated with the gateway that is accessible to the server.

9. The method according to any of the preceding claims, wherein the gateway requests the server for issuance of a new credential token if the credential token is inactive.

10. The method according to any of the preceding claims, wherein the unique identifier of the gateway is generated from MAC address and product ID.

11. A system for managing secure communication remotely between a device coupled to a gateway and a server, the system comprising:
the server comprising:
a processor; and
a data management module configured to:
generate a unique identifier based on encrypted data received from the gateway;
authorize a gateway based on the unique identifier;
provide a credential token associated with the gateway for use in communications between the gateway and the server;
generate a key for the device that is authorized to communicate with the server; and
manage communication between the server and the device; and
the gateway comprising:
a processor;
a communication interface for receiving and sending data from the device; and
a network module configured to:
provide the unique identifier for communicating with the server;
receive the credential token for communicating with the server; and

authorize the device for communicating with the server based on the generated key associated with the device,

wherein the server, the gateway, connects to the device, obtains data from the device and sends the data to the server via the communication interface to manage the data received from the device remotely.

12. The system according to claim 11, wherein the server comprises a pool of the unique identifiers.

13. The system according to any one of claims 11 or 12, wherein the server is in communication with a plurality of gateway.

14. The system according to any one of claims 11 to 13, wherein the device is coupled to the gateway by physical ports or wireless communication.

15. The system according to any one of claims 11 to 14, wherein the gateway is encrypted.

16. The system according to claim 15, wherein the gateway is configured to create and store a decryption key that is accessible to the server device.

17. The system according to any one of claims 11 to 16, wherein the gateway requests the server for issuance of a new credential token if the credential token is inactive.

18. The system according to any one of claims 11 to 17, wherein the unique identifier of the gateway is generated from MAC address and product ID.

19. The system according to any one of claims 11 to 18, wherein the system is configured for adopting and integrating by the server and/or the one or more devices.

20. The system according to claim 19, wherein the system is configured to provide centralized management of the one or more devices remotely.

21. The system according to any one of claims 11 to 20, further comprising a network communication means configured to allow transmission between the server and the device.